Malicious infrastructure as a service

silentpush.com/blog/malicious-infrastructure-as-a-service

April 25, 2021

Apr 25
Written By Ken Bagnall

Martijn April 13th 2021

Domains created for malicious purposes are rarely registered on their own. When you have identified such a domain, it is therefore always a good idea to look for other domains used in the same campaign.

Sometimes finding such a domain is easy. For example, you may notice a very similar domain (such as the .net version of a .com domain) registered with the same registrar on the same day. At other times you will need to look for other evidence, for example find them hosted on the same IP address.

In general, however, linking two domains through a single IP address isn't strong enough evidence that the domains themselves are linked. The link becomes a lot stronger though when two or more domains were seen moving through the same set of IP addresses

simultaneously.

In previous blog posts, I used this to find five domains that used the same infrastructure and that were made to look like they belonged to a content delivery network, as well as the infrastructure of a LodaRAT campaign targeting Bangladesh.

In this blog post, I will share a few more examples of sets of malicious domains that moved simultaneously through the same set of IP addresses. The sets of domains are linked and there is some evidence to suggest that the infrastructure belongs to a bulletproof hosting service.

Magecart

The first set of domains spoofs well known services such as Cloudflare, Google, jQuery and Magento:

```
cloudflareplus[.]com
cloudflareplus[.]net
cloudflareshop[.]com
cloudflare[.]su
googleexpert[.]name
googleinfo[.]name
googlemanagerads[.]com
googlemaster[.]name
googleplus[.]name
gooqlescript[.]com
jquery24[.]com
jqueryexpert[.]com
jqueryinfo[.]com
jquery[.]su
jsstroy[.]com
magentoinfo[.]name
magentoinfo[.]org
magentoportal[.]com
magentostore[.]org
manualseos[.]ru
mycloudflare[.]net
procloudflare[.]com
procloudflare[.]net
seocmson[.]ru
```

These domains were all registered at Russian registrar REG.RU on the 3rd of November 2020 and have simultaneously moved through the same set of IP addresses. The all use the name servers of DNSPod, a Chinese DNS hosting provider that has long been popular with cyber criminals.

For the first three months of 2021, the domains were seen on the following twenty IP addresses, in this order:

```
208.69.117[.]117
194.147.78[.]6
45.143.136[.]186
92.38.130[.]71
46.17.250[.]52
46.17.250[.]84
91.203.192[.]117
34.65.156[.]213
35.189.71[.]51
34.65.43[.]209
35.197.218[.]54
35.205.161[.]91
8.209.112[.]138
35.228.62[.]27
34.107.33[.]136
35.228.209[.]29
35.187.16[.]185
35.228.228[.]1
35.204.191[.]93
35.198.110[.]173
```

Sometimes, the domains only pointed to an IP address for less than a day, but in one case they pointed to the same IP address for three weeks in a row.

The IP addresses belong to various hosting services, with a particular preference for Google's.

Interestingly, around the 8th of March, nine more domains joined the cycle:

```
bing-visitors[.]com
cloubfiare[.]net
googiemanager[.]com
googlemanagerads[.]com
googlemgr[.]net
googletag[.]name
gooqleads[.]net
qodaddy[.]net
yahoo-tracker[.]com
```

They have been pointing to the same IP address as the original set ever since.

There is public evidence linking these domains to Magecart. Magecart is an umbrella term use to refer to more than a dozen groups that insert code into websites' payment pages that steals credit card data. A common trick used by Magecart groups is to make their domains look like those from which code is regularly included into web pages. A website owner looking at a web page's source code may thus incorrectly assume the inclusion of third-party JavaScript is harmless.

Note: because the domains sometimes pointed to an IP address for a very short time period, it is possible that the list of IP addresses above isn't complete for the three-month period January 1st to March 31st 2021. The same applies to the examples below.

IcedID and Qakbot

A second set of domains also cycled through a set of IP addresses, again all pointing to the same IP address at the same point in time.

The domains are:

aath22rzmo03mvewdj[.]xyz
amr16pzcp03omerd[.]xyz
caqp10snyod03msvsqu[.]com
fkko03vvxohq03taep[.]com
cidn02mjco03pobx[.]com
cyh26wcekai02atpeax[.]com
drt22uhfjmz03ltxc[.]xyz
dskl02touc03jeby[.]com
dzw10jpcgj03fckc[.]com
emqjj27ljgl02hqqzi[.]com
etysu02scnabr03wzaxue[.]com
evz15lmlir03sygmyr[.]xyz
b25d3a23hy[.]com
fb25d3add23hy[.]com
fb25d3as23hy[.]com
fb25d3asddd23hy[.]com
fb25d3erda23hfy[.]com
fb25era23hfy[.]com
fb25erhfy[.]com
ftkaq03ihfbh03rehx[.]com
fyz10eijkl03mytjfb[.]com
gbza26rngn02bekll[.]com
ghtyrncjf2df[.]com
hei03tfxv03mahl[.]com
hqcaz02egeq03bvmhm[.]com
hqn27dyhvwp02wznv[.]com
ihjpn03sijjl03dtmtr[.]com
inpa02lzjvt03anas[.]com
jam03iofwv03jniedf[.]com
jgu16cbxdr03ehqvx[.]com
jhj10jtvwu03zsjwk[.]com
jqilt27xsbz02anaeu[.]com
klhlh16zldwun03vlpq[.]com
kyvws03ndah03hecon[.]com
lic02uiccnh03nruvp[.]com
lxoyw10bipu03ilyig[.]com
mtk23gqakwj03bzds[.]xyz
qnvrih26coxejl02enyfn[.]com
nwvv27dwmy02bgznc[.]com
nygvj27cvlk02cktf[.]com
olfs23kvri03wyyb[.]xyz
ououz02naba03oiyd[.]com
pbdq26xjey02uprxwx[.]com
ppk02dmgmzj03dxekog[.]com
qab26utxb02pquc[.]com
rdraj16rwjw03xnli[.]com
rea26ypgvle02hcbunp[.]com
rlvq27rmjej02sfvb[.]com
rlyrt26rnxw02vqijgs[.]com
rsjb23tnxjng03dgiy[.]xyz
sal03gicu03qcwtif[.]com
tmrz10fxhy03ntxjf[.]com
toj27nlpr02irajz[.]com
toqku26hwpu02shuroh[.]com
ttj10qrrqx03kdts[.]com

```
usy15wycqme03dymh[.]xyz
vad12mhpfp03vyfl[.]xyz
vdk10pfsny03tzfva[.]com
vpu03jivmm03qncgx[.]com
vyhml26anpfyb02aqsehz[.]com
vyw27lfrvoj02kkxo[.]com
wnah27frybfe02sadb[.]com
xgka03stox03cloeqz[.]com
xjw10whta03ytgdi[.]com
xsd22aeofw03lqzf[.]xyz
yar03jmtvr03jtqg[.]com
ydw27hfhbk02zpidmv[.]com
ywgiu10zmnwcx03vpnyp[.]com
zkkn02lffiff03zkmh[.]com
```

while the IP addresses are

```
47.254.134[.]0
34.90.237[.]156
8.209.64[.]96
8.209.68[.]209
34.89.57[.]175
8.208.97[.]177
35.228.62[.]27
8.210.31[.]137
35.228.48[.]27
34.65.218[.]17
8.209.98[.]100
35.204.191[.]93
8.211.4[.]209
```

The domains were registered between late February and mid March 2021, mostly through Dutch registrar Hosting Concepts with a few using REG.RU instead. The nameservers used were again those of DNSPod, while the IP addresses belong to Google and Alibaba.

Interestingly two of the IP addresses (marked in bold above) were also used by the Magecart domains above, suggesting a possible link between the two sets.

Many of the above domains have been used to download either the IcedID or the Qakbot malware. Both IcedID and Qakbot (also known as Qbot) are commonly used as initial access brokers. Though no direct link between these two actors is known, recently URLs of the type that previously served Qakbot started to serve IcedID instead.

This suggests that it is another actor that handles the spam campaigns that delivers either malware, an example of the increased commoditization of cybercrime. This would also explain why the domains listed above are different from the IcedID command and control domains I wrote about recently., which use a different hosting infrastructure.

Ursnif and phishing

A third set of domains also cycled through a set of IP addresses:

```
aodacrtsrytuce[.]com
ashguq[.]com
chonlinedocstorage[.]com
companieshdocstorage-online[.]com
docusign-cloudab[.]com
docusign-cloudbc[.]com
docusign-cloudcd[.]com
docusign-cloud[.]com
docusign-vault[.]com
edssrdsceaaorb[.]com
exhssppceaaorb[.]com
hutnspiekeagrm[.]com
ioqpuyfshaio[.]com
ipqweyb[.]com
jyohjdowprwiondotrbkght[.]com
nbmipqw[.]com
ospzsiq[.]com
qpofsgw[.]com
rconalacrtnspi[.]com
rvprmsrirdeala[.]com
srirdelehssfaojr[.]com
srtnserqdelaeh[.]com
uidacrtsppxece[.]com
uiwoqp[.]com
upsdocstorage[.]com
upsdocstorage-online[.]com
vcavwq[.]com
wvmiap[.]com
zhdipqw[.]com
```

The IP addresses in this case are:

```
188.227.58[.]120
45.143.136[.]43
188.227.86[.]64
91.203.192[.]117
35.228.188[.]33
35.246.93[.]71
35.228.88[.]152
```

All these domains were registered through Eranet, a registrar based in Hong Kong, and again used DNSPod's nameservers. Two of the IP addresses, marked in bold, were also used by the Magecart domains, suggesting a possible link.

Interestingly, there are two kinds of domains in the list. One the one hand, there are random looking domains which, as with the IcedID/Qakbot domains above, could suggest a domain generation algorithm (DGA). On the other hand, domains like docusign-cloud[.]com and upsdocstorage[.]com of which one can be all but certain they have been used in phishing campaigns: both DocuSign and UPS are commonly used in phishing lures.

It is not surprising therefore that these latter domains were taken down, often within a week after becoming active: lookalike domains are actively hunted by the affected organisations.

As for the DGA-like domains, one of them, uidacrtsppxece[.]com, has been linked to Ursnif, another common malware delivered in email campaigns.

It is unclear whether there is a direct link between Ursnif and the phishing domains beyond the use of the same infrastructure, or even whether all DGA-like domains have served Ursnif.

Other domains

There are many other domains that have used the same infrastructure, including the use of the DNSPod DNS provider.

For example, the domains

```
ie-kbc[.]net
ie-kbc[.]org
kbc-ie[.]net
www.kbcbanking[.]net
```

will no doubt have been used to impersonate KBC, an Irish bank, while authorise-eebilling[.]com has likely targeted customers of UK mobile provider EE. There are also several more domains that suggest a DGA.

Conclusion: a bulletproof hosting provider?

The similarities among the various sets described above, such as the use of DNSPod and the sharing of IP addresses, suggests the campaigns described all use the same infrastructure, likely that of a bulletproof hosting service.

A bulletproof hoster serves a similar function as a content-delivery network (CDN) does for legitimate domains: making it harder for a denial-of-service attack. The “attack” in this case would come from law enforcement and security researchers.

In the past, bulletproof hosters ran their own networks, which often led to the whole ASN being blocklisted. More modern bulletproof hosters rent servers at cloud providers and set these up as proxies for their customers’ content. By rotating through a set of IP addresses, the content is less vulnerable to being blocked based on the IP address.

Intel471 recently wrote about bulletproof hosters and in particular mentioned DNSPod.

Of course, we cannot be 100% certain that this is a bulletproof hoster, or even that the various campaigns do use the same infrastructure: the sharing of IP addresses may be a coincidence, or because there is another party involved in renting the servers.

But this is yet another example that shows how understanding the context of a domain name can help one find a lot of related infrastructure that is worth blocking, even without having seen evidence of actual malicious activity.

Subscribe

Sign up with your email address to receive news and updates.

We respect your privacy.

Thank you!

Ken Bagnall